UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,103	06/30/2000	Christopher L. Hamlin	K35A0631	1085

26332 7590 01/27/2005

WESTERN DIGITAL CORP.
20511 LAKE FOREST DRIVE
C205 - INTELLECTUAL PROPERTY DEPARTMENT
LAKE FOREST, CA 92630

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/608,103	HAMLIN, CHRISTOPHER L.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 November 2004* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. In response to communications filed on 11/15/2004 for a continuation of examination, the following claims 1-16 are presented for examination.

2. Applicant's remarks, pages 9-12, filed on 11/15/2004, with respect to the rejection of claims 1-16 have been fully considered, and they are persuasive. Upon further consideration a new ground of rejection is made in view of Sohne in combination to Spies et al.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1 **Claims 1-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,397,333 to **Sohne et al.** in view of US Patent 6,230,269 to **Spies et al**.

3.2 **As per claims 1 and 9, Sohne et al.** substantially teaches a secure disk drive comprising: a memory for storing data (see column 4, line 64); (b) an input for receiving an encrypted message from a client disk drive, the encrypted message comprising ciphertext data and a device ID (see column 3, lines 8-11); (c) (d) **Sohne et al** also discloses public/private key pairs (column 3, lines 30-60) that meets the recitation of secure key and internal drive ID; (e) generating master key from public/private key pairs that meets the recitation of generating an internal drive key based on the internal drive ID and the secure drive key; (f) an authenticator for verifying the authenticity of the encrypted message and generating an enable signal, the authenticator responsive to the encrypted message and the client drive key (see column 3, lines 60-64); (g) a data processor comprising: a message input for receiving the encrypted message from the client disk drive; a data output for outputting the ciphertext data to be written to memory that meets the recitation of written to disk (see column 4, lines 60-64); a data input for receiving ciphertext data read from the disk (see drawings); an enable input for receiving the enable signal for enabling the data processor (see column 4, lines 44-47 and lines 64-67); a key input for receiving the internal drive key (see drawings). **Sohne et al.** does not explicitly teach authenticating using a drive ID to identify the host; generating client drive key based on client drive ID and secure drive key; and generating message authenticating code. However, **Spies et al** discloses a secure distribution system wherein the client construct a message containing hash value with the user ID and a randomly session key that meets the recitation of (b) an input for receiving an encrypted message from a client disk drive, the encrypted message comprising ciphertext data and a client drive ID identifying the client disk drive (see abstract). **Spies et al** further discloses the teaching of public/private key pairs in both the server and the client for encryption of the message to

allow bilateral authentication (column 6, lines 19-26), and the server generates key source material based on the client information (column 8, lines 55-58) that meets the recitation of generating client drive key based on client drive ID and secure drive key. **Spies et al** discloses key input for receiving ID and password for generating message authentication code (column 5, lines 30-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Sohne et al** to implement the inventive concept of **Spies et al** in authenticating both parties transmitting the encrypted message using bilateral authentication and message authentication code. This modification would have been obvious because one skilled in the art would have been motivated to authenticate both the sender and the receiver to guarantee that the message originates from the right sender and preventing attacks as suggested by **Spies et al** (column 6, lines 47-63).

As per claims 2 and 10, Sohne et al. discloses the limitation of using a secure drive key that is immutable (see column 3, lines 37-38).

As per claims 3 and 11, Sohne et al. discloses the limitation of using a secure drive key that is mutable (see column 3, lines 19-23).

As per claims 4 and 12, Spies et al discloses means for verifying both parties that meets the recitation of wherein the authenticator comprises means for verifying the access rights of the client drive ID (see abstract and column 6, lines 28-30). Therefore claims 4 and 12 are rejected on the same rationale as the rejection of claim 1.

As per claims 5-7 and 13-15, the limitation of wherein the secure drive key, key generator and authenticator comprising tamper resistant circuitry are well known in the art **Sohne et al.** discloses using the term device can be any storage including multimedia card (column 4, lines 43-48).

As per claims 8 and 16, Sohne et al. discloses the limitation of wherein the data processor further comprises cryptographic facilities (see column 4, lines 35-67).

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin
Patent Examiner
January 21, 2005